

**REMARKS**

In the December 1, 2005 Office Action, the Examiner noted that claims 1, 6, 24, 27 and 34-37 were pending in the application; rejected claims 1, 6 and 34-37 under 35 USC § 102(e); and rejected claims 24 and 27 under 35 USC § 103(a). In rejecting the claims, U.S. Patents 5,689,567 to Miyauchi (Reference A in the June 3, 2005 Office Action) and 6,292,092 to Chow et al. (Reference A in the June 16, 2004 Office Action) were cited. Claims 38-53 have been added and thus, claims 1, 6, 24, 27 and 34-53 remain in the case. The rejections are traversed below.

**Rejections under 35 USC § 102(e)**

In items 3-7 on pages 2-4 of the Office Action, claims 1, 6 and 34-37 were rejected under 35 USC § 102(e) as anticipated by Miyauchi. These rejections were substantially the same as in the June 3, 2005 Office Action, except for changes reflecting the amended and added claims and citation of additional portions of Miyauchi (column 3, line 52 to column 4, line 24 and column 6, lines 1-3, 10 and 11). The newly cited portions relate to use of signature documents, specifically signature image G which "is digital information of ... a print of a seal or a written signature" (column 3, lines 15-17) that "is encrypted with a key of the hash value H corresponding to a secret-key cryptosystem" (column 3, lines 31-33). Further encrypting and decrypting are described, ending with "the signature image ... generated according to the decryption function  $G=f_2(B,H)$ " (column 6, lines 1-3).

Item 12 on page 6 of the Office Action was entitled "Response to Arguments" but failed to respond to the arguments in the Amendment filed by certificate of mail on September 6, 2005 (received by the U.S. Patent and Trademark Office September 8, 2005). Instead, item 12 of the Office Action repeated that column 4, line 62 to column 5, line 12 of Miyauchi discloses a "hash value generated from a signature object document M, and further encrypt[ing] the signature image G with a key of the hash value" (Office Action, page 6, lines 7-8). This statement fails to rebut the point of the argument in the paragraph spanning pages 5 and 6 of the September 6, 2005 Amendment, namely that what supplied to the receiving side of the system disclosed by Miyauchi is not everything that is recited in claim 1 as included in the output of the signature system.

As noted in **bold** letters in the September 6, 2005 Amendment, claim 1 recites that what is output by a signature system according to the invention is "output information including a signature **program**" (claim 1, line 5), where the signature program is used to generate "first blind information from illegal use prevention information ... and ... both the first blind information and

the illegal use prevention information [are included] in the signature information" (claim 1, last 3 lines). As stated in the September 6, 2005 Amendment, "[n]othing was cited in Miyauchi suggesting that the MD5 message-digest algorithm or any encryption program is obtained from a 'system presenting a receiver with signature information of a user' (claim 1, lines 1-2)." In other words, Miyauchi fails to teach a system that outputs the **program** used to produce the signature information, so that this program can be used by a receiving system in authenticating the signature.

As previously recited in claim 1, "the signature program generates first blind information from illegal use prevention information for protection against illegal use, and enters both the first blind information and the illegal use prevention information in the signature information" (claim 1, lines 6-8). Thus, blind information of illegal use prevention information is created from the illegal use prevention information, e.g., using a hash function and an encryption key of the illegal use prevention information, as described on page 16 of the application, for example. This permits verification that the receiver device has read the "output information," such as a two-dimensional bar code from a user device, as described on pages 13-15, for example.

To provide the receiver device which reads the two-dimensional bar code with an algorithm for generating the blind information, the signature system recited in claim 1 "the output information include[es] a signature program" (claim 1, line 5), e.g., the signature program is embedded into the two-dimensional bar code, so that the receiver device can generate the blind information. Although the application discloses an algorithm for generating the blind information employing an MD function and an encryption key, the claims are not so limited and any signature program can be included in the output information, e.g., "format readable by a bar code reader" (e.g., claim 24, lines 9-10), so that the blind information generation algorithm can be loaded in the receiver device, which has never possessed the algorithm before, by reading the output information, e.g., a two-dimensional bar code.

In the Office Action it is asserted that Miyauchi discloses the blind information generation algorithm. Even if there is similarity of the generation algorithms, Miyauchi does not describe anything about including the signature program in the output information, as recited in claim 1. In other words, the description of Miyauchi is under a premise that the receiver possesses a hash function and a public key. It does not describe how the receiver obtains the hash function and the public key.

Since there is no such description in Miyauchi, the feature of the present invention that the signature program for generating the blind information from the use information is included in output information (e.g., in a two-dimensional bar code) is not disclosed by Miyauchi.

In addition, Miyauchi does not teach or suggest that "after the signature information is generated according to the output information to present the signature information to the receiver, the signature program can be removed from memory" (claim 1, last 3 lines). Embedding the signature program and disposing of it after use, as recited in claim 1, is an essential feature to prevent the abuse of the output information of the user device by the receiver device and a third party. Since Miyauchi does not describe any way to obtain the blind information generation algorithm or disposal of the algorithm after the generation of the blind information, it is submitted that claim 1 and the other independent claims reciting similar limitations patentably distinguish over Miyauchi.

For the above reasons, it is submitted that claim 1 patentably distinguishes over Miyauchi. Since claim 6 depends from claim 1, it is submitted that claim 6 patentably distinguishes over Miyauchi for at least the reasons discussed above with respect to claim 1.

Claim 34 has been amended to depend from new claim 45 and therefore will be addressed below.

With respect to claim 35, item 4 of the December 1, 2005 Office Action asserted that registering one-directional functions to specific users (see claim 35, line 3) for "generating second blind information from the authentication information contained in the signature information, using the one-directional function" (claim 35, lines 6-7) was disclosed at column 4, lines 37-67 and column 5, lines 39-61 of Miyauchi. However, these portions of Miyauchi merely describe means for input of a signature image and secret information of the signer. There is no suggestion that this is not being done in real time by the signer or the existence of a "management unit for managing first blind information generated from authentication information, one-directional function and encryption key which are registered by a user" (claim 35, lines 2-3).

To protect user information security, even a certification device does not store the original authentication information of a user, but stores blind information alone. For that reason, the blind information is generated from authentication information received from the receiver device and the generated blind information is compared with the stored blind information. In Miyauchi, received information is decrypted as in the conventional art, and is compared with the original image information G. Hence, the technical mechanism of the present invention, in which

the certification device generates blind information by itself and compares with the stored blind information, is not described at all.

In a certification device according to the present invention, the user device also registers the blind information and the one-directional function and encryption key to generate the blind information, and the authentication information is not stored in the certification device. Thus, for the reasons set forth above and in the September 6, 2005 Amendment, it is submitted that claim 35 patentably distinguishes over Miyauchi and Chow et al.

Neither item 7 setting forth the rejection of "claims 35-37" nor the "Response to Arguments" addressed the arguments in the September 6, 2005 Amendment regarding the patentable distinctions of claims 36 and 37 over Miyauchi. Therefore, it is submitted that claims 36 and 37 patentably distinguish over Miyauchi and Chow et al. for the additional reasons set forth in the September 6, 2005 Amendment.

#### **Rejections under 35 USC § 103(a)**

Claims 24 and 27 recite additional details regarding how the program used in generating the signature information is output from the system that generates the signature information. For example, claim 24 recites "generating output information for generation of signature information of the user according to the input identification information" (claim 24, lines 4-5), then "outputting the output information and the signature program in a format readable by a bar code reader" (claim 24, last 2 lines). Claim 27 similarly recites "outputting information for generation of the signature information according to the input identification information, including a signature program, in a format readable by a bar code reader" (claim 27, lines 4-6).

The "Response to Arguments" in the December 1, 2005 Office Action did not address the argument in the September 6, 2005 Amendment that Chow et al. fails to teach or suggest "modifying the system taught by Miyauchi to record a **program** in a bar code or to output any kind of program in any way" (September 6, 2005 Amendment, page 6, lines 30-31). It is this lack of teaching in the combination of Miyauchi and Chow et al. that was the thrust of the arguments in the September 6, 2005 Amendment, not a generic failure to suggest combination of the references as asserted in the "Response to Arguments" in the December 1, 2005 Office Action.

As noted in the September 6, 2005 Amendment, the cited portion of column 4 of Chow et al. only describes a "combination of ... personal information and a digitized descriptor of the photograph and/or personal information ... which after encrypting ... is recorded" (column 4, lines 62-65), e.g., as a "two-dimensional bar code" (column 3, line 1). The cited portion of

column 7 of Chow et al. similarly describes a "fixed number, which is a digitized descriptor of the photograph (and/or personal signature if used), [that] is ... combined with the digitized personal information or code resulting from the hash function processed personal information, is encrypted and is fixed to the card" (column 7, lines 57-62). Thus, Chow et al. fails to teach or suggest outputting a program in a bar code and since Miyauchi fails to teach or suggest outputting the program used to generate the signature information, the combination of Miyauchi and Chow et al. fails to teach or suggest the limitations recited in claims 24 and 27.

### **New Claims**

New claim 38 depends from claim 37 (and thus, claims 35 and 36) and new claims 41 and 42 depend from claim 1. Therefore, it is submitted that claims 38, 41 and 42 patentably distinguish over the prior art for the reasons discussed above with respect to the claims from which they depend.

Claim 50 recites "reading information in a bar code format, including program information, for generation of signature information" (claim 50, lines 3-4). As discussed above, neither Miyauchi nor Chow et al. teaches or suggests providing program information in this manner. Therefore, it is submitted that claim 50 and claim 52 which recites a similar limitation patentably distinguish over Miyauchi and Chow et al. for at least this reason.

Claim 51 recites "managing first blind information generated from authentication information, a one-directional function and an encryption key which are registered by a user" (claim 51, lines 3-4). As discussed above with respect to claim 35, neither Miyauchi nor Chow et al. teach or suggest such an operation. Therefore, it is submitted that claim 51 and claim 53 which recites a similar limitation patentably distinguish over Miyauchi and Chow et al. for at least this reason.

### **Summary**

It is submitted that the references cited by the Examiner, taken individually or in combination, do not teach or suggest the features of the present claimed invention. Thus, it is submitted that claims 1, 6, 24, 27 and 34-53 are in a condition suitable for allowance. Entry of the Amendment, reconsideration of the claims and an early Notice of Allowance are earnestly solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Serial No. 09/771,896

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 3/1/06

By: Richard A. Gollhofer  
Richard A. Gollhofer  
Registration No. 31,106

1201 New York Avenue, NW, Suite 700  
Washington, D.C. 20005  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501